Privacy Encryption Antivirus

Home / Security

Widely used SHA-1 algorithm could succumb to attack, researchers warn

It's time to retire the SHA-1 hashing algorithm, as it is now cheaper than ever to attack, researchers say

A padlock icon in the browser's address bar indicates that a secure HTTPS connection has been established with a server by means of an SSL certificate from an acceptable certification authority (CA). Credit: Peter Sayer

COMMENTS

Peter Sayer
IDG News Service

Oct 8, 2015 8:29 AM

Researchers have found a new way to attack the SHA-1 hashing algorithm, still used to sign almost one in three SSL certificates that secure major websites, making it more urgent than ever to retire it, they said Thursday.

from our new site, Greenbot

Apple pushes into virtual reality by hiring top VR expert

Backdoor account replaced by another backdoor

SHA-1 is a cryptographic hashing function designed to produce a fingerprint of a document, making it easy to tell if a document has been modified after the fingerprint was calculated.

Weaknesses had already been identified in SHA-1, and most modern Web browsers will no longer accept SSL certificates signed with it after Jan. 1, 2017. That date was chosen based on the ever-decreasing cost of the computing power required to attack the algorithm.

The researchers who developed the latest attack, though, think SHA-1 should be phased out sooner, as they estimate it now only costs between $75,000 and $120,000 to mount a viable attack using freely available cloud-computing services. Previously, Intel researcher Jesse Walker had estimated it would take until 2018 for the cost to reach this level, which he suggested was well within the reach of criminal syndicates.

Coincidentally, the Certification Authority/Browser Forum, which agrees policies on support for SSL certificates, is examining proposals to continue issuing SSL certificates signed with SHA-1 beyond the previously agreed cut-off date. Certification Authorities (CAs) issue and vouch for certificates used to secure websites.

The researchers said they strongly recommended that proposal be rejected.

Hashing agorithms like SHA-1 are considered secure if it is vastly more difficult to create a document that matches a given hash than it is to calculate a hash from a given document.

If someone can create two different files that have the same hash, it’s possible to digitally sign one—say, a benign downloadable app—and then later replace it with a malicious one in a way that electronic audit trails would be unable to identify. This is called an identical-prefix attack.

Even more serious is if someone can take an existing document with a known hash, and create a new file matching that hash, a so-called known prefix attack. This would allow the undetectable replacement not only of apps identified by their hashes, but also of SSL security certificates signed with them.

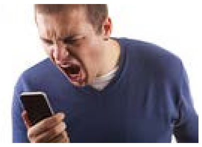
The attack on on SHA-1’s compression function was described by Thomas Peyrin of Nanyang Technological University (NTU) in Singapore, Marc Stevens of the Centrum Wiskunde and Informatica in the Netherlands and Pierre Karpman of both NTU and Inria in France. It goes through the message block by block, calculating a hash for each block combined with the hash derived from all the previous blocks. In SHA-1 this is done in 80 “rounds”, and the three say that their attack is the first to break all 80 rounds.

Happily, the researchers have only shown a way to simplify an identical-prefix attack on SHA-1, meaning it is not yet possible to generate fake SSL certificates allowing the impersonation of arbitrary websites.

“This is still far from being able to create a rogue CA, as such an attack would require a stronger type of collision,” said Peyrin, one of the authors of the research paper.

in security...

12 gorgeous PC games that will punish your graphics card



10 texting habits you need to break

"We advise the industry to not play with fire, and accelerate the migration process toward SHA2 and SHA3, before such dramatic attacks become feasible," Peyrin concluded.

Related: Security

Peter Sayer Paris Bureau Chief

Peter Sayer covers open source software, European intellectual property legislation, and general technology breaking news for the IDG News Service.

More by Peter Sayer

COMMENTS